DECLARATION OF SPECIAL AGENT ERIC HISER

I, Eric Hiser, do hereby declare:

Agent Background and Training

1. I am a Special Agent with the Federal Bureau of Investigation and have been since April 11, 2021. My current assignment is with the Portland Field Office on the White Collar Crimes squad investigating financial crimes. My training and experience includes twenty-one weeks of specialized training received at the FBI Academy in Quantico, Virginia, related to investigative and legal matters. During that time, I was taught the use and practical application of authorized investigative techniques. I also previously worked as a forensic accountant from 2016 to 2020 in the FBI's Philadelphia Division, where I assisted FBI special agents with the investigation of organized crime, money laundering, and fraud.

Purpose of Declaration

2. This declaration is submitted in support of a complaint for forfeiture. The information contained in this declaration is based on an investigation I conducted, which will show 3,086,213.86 Tether (USDT) seized from a Binance account with User ID 111213443 held in the name of Nan Song **(Binance-Song 3443)** and 3.41 Bitcoin (BTC), or equivalent cryptocurrency, valued at approximately $331,051.05 on December 9, 2024, stored in an OKX account with User ID 460511322279437347 held in the name of Yao Lutao (**OKX-Lutao 7347**) were involved in transactions or attempted transactions or traceable to money laundering offenses in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) and 18 U.S.C. § 1957 (unlawful monetary transactions in excess of $10,000), and is property constituting or derived from proceeds obtained, directly or indirectly, from a violation of 18 U.S.C. § 1343 (wire fraud). These funds are

subject to seizure pursuant to 18 U.S.C. §§ 981(b) and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) & (C).

3. The facts set forth in this declaration are based on my own personal knowledge; knowledge obtained from other individuals during my participation in this investigation, including other law enforcement officers; FBI forensic accountants; interviews of witnesses; my review of records related to this investigation; communications with others who have knowledge of the events and circumstances described herein; and information gained through my training and experience. This declaration does not set forth each and every fact that I or others have learned during the course of this investigation, only those necessary to establish probable cause to believe the cryptocurrency described within is subject to seizure pursuant to 18 U.S.C. § 981(b), and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) and (C).

Summary of Investigation

4. The Federal Bureau of Investigation (FBI) is investigating a cryptocurrency investment fraud scheme conducted by a transnational criminal organization. The FBI received information from a victim who claimed to have lost approximately $900,000 in a cryptocurrency investment fraud scheme through the platform Bitnukes. The FBI conducted blockchain tracing using commercially available tools and identified a series of cryptocurrency wallets and cryptocurrency exchange[1] accounts used to facilitate the theft of the victim's funds and subsequent laundering. At least eight additional victims located across the United States reported to the FBI

[1] Cryptocurrency exchanges are platforms that facilitate the trading of cryptocurrencies for other assets, including other cryptocurrencies and fiat currency. Cryptocurrency exchanges mentioned in this declaration include Crypto.com, Kraken, Binance, OKX, HTX, and MEXC.

that they lost a combined $1,580,798 through the Bitnukes' platform. Blockchain tracing indicates the scheme could exceed 460 BTC, valued at approximately $44,646,284.40 as of December 9, 2024. FBI forensic accountants traced likely proceeds of fraud to two accounts held at two cryptocurrency exchanges, which were targets of previously issued seizure warrants (3:24-mc-901).

Statement of Probable Cause

5. In long-term cryptocurrency investment fraud schemes, perpetrators generally meet victims online and establish an emotional connection and trust with victims to provide them with a false sense of security. The relationships established can vary from platonic to intimate. Victims then learn about an investment opportunity from the perpetrator and are presented with an opportunity to invest. Victims generally start their investment small and earn a high rate of return, which they are encouraged to withdraw from the platform. Victims often withdraw these funds successfully.

6. Once victims are comfortable with the investment process and platform they are pressured to invest larger sums of money. Some victims liquidate retirement accounts and invest their life's savings. Victims can view the investment's substantial growth through an online portal. Trouble begins after victims have invested a large amount of money and attempt to withdrawal their fictitious gains. Victims are often instructed the money is frozen due to taxes owed on the profit, which cannot be withheld from the investment proceeds. At this point, some victims pay the taxes and never receive their money. Others realize they have been scammed, and some contact law enforcement. These schemes can be devastating for victims because not only can they lose a substantial amount of money, but they are tricked by someone they thought was a good friend or intimate partner.

Oregon Investigation – Victim 1

7. On April 25, 2023, Victim 1, a resident of Oregon, went to the FBI Portland Field office to report that he was a victim of a cryptocurrency investment fraud scheme. Victim 1 told FBI agents that on March 9, 2023, he met Mia Tara on Twitter. Tara claimed be a cryptocurrency investor who lived in New York. Tara told Victim 1 she could teach him how to become a successful cryptocurrency trader through a trusted mobile application called Bitnukes, which Tara claimed was owned and operated by Tara's aunt, a cryptocurrency data analyst. Tara befriended Victim 1 and even gave him her father's phone number, so he could call her father if Victim 1 ever feared Tara was in trouble.

8. Tara eventually encouraged Victim 1 to transfer money to Crypto.com to trade on the platform Bitnukes, URL bnukeskp(.)vip. On March 17, 2023, at Tara's direction, Victim 1 sent .04 BTC valued at approximately $972.90, on the date of the transfer, to a cryptocurrency wallet provided by Tara to invest. Victim 1 told FBI Agents that he made money on the investment and transferred it back to an account under his control at the direction of Tara.

9. Feeling comfortable with Bitnukes, from March 28 to April 21, 2023, Victim 1 transferred an additional 30.79 BTC for a total investment of approximately 30.83 BTC, valued at approximately $878,291.61 at the time of investment. Victim 1 watched his funds grow on the investment platform's website. A special bonus was available for accounts that invested more than $1 million. Victim 1 was close to meeting the $1 million bonus level, so Tara even purportedly contributed her own money directly to the platform so that Victim 1 could obtain the bonus.

10. Victim 1 trusted Bitnukes because of Tara. At some point, Victim 1 and Tara's relationship turned intimate. I reviewed WhatsApp messages between Victim 1 and Tara from as

early as April 13, 2023, which indicated the relationship between Victim 1 and Tara by that point was intimate in nature. In a message on April 16, 2023, Victim 1 referred to Tara as his soulmate and Tara replied, "Yes, we are a team, we are soul mates, we are lovers." Victim 1 never met Tara in person.

11. On April 14, 2023, Bitnukes' server went down. Victim 1 told Tara, and she provided him with a new website, exskaocc(.)one. With this new website, Victim 1 was able to view his account again. By April 21, 2023, Victim 1's investment of approximately $878,291.61 was valued at approximately $2.9 million and Victim 1 initiated a withdraw for the entire account balance. The withdrawal triggered an automatic freeze that Tara told Victim 1 was normal due to taxes owed on Victim 1's gains. Tara directed Victim 1 to chat with Bitnukes customer service to resolve the freeze.

12. On April 23, 2023, Victim 1 chatted with Bitnukes customer service and was told that he owed $557,959 on the gains that could not be withheld from his profit or principal. Later in the day, Victim 1 chatted with a customer service manager and was told there was no way to unfreeze the funds until the taxes were paid. Tara offered to help, but she told Victim 1 she could only contribute $150,000. At this point, Victim 1 realized he was scammed and never paid the taxes or received his money back.

13. On December 1, 2023, Victim 1 filed a civil complaint in the United States District Court for the Northern District of Florida against Tara and others. Victim 1 notified the defendants of the civil complaint via WhatsApp, and according to court records Tara confirmed receipt of the legal process. The defendants failed to appear, plead, or defend in the suit, so the court granted Victim 1 a final judgment for $1,373,897 on February 5, 2024. The final judgment

amount reflected appreciation in BTC's value from the date of Victim 1's initial investment. Court records indicate no payments have been received as of December 9, 2024.

▼Judgments

Date	In Favor Of	Against	Amount	Interest	Court Cost	Status	Status Date
02/05/2024	V1	DEFENDANT "1"	$1373897.97	0.00%	$ 0.00	No Payment	02/05/2024
02/05/2024	V1	JOHN DOES 1-20	$1373897.97	0.00%	$ 0.00	No Payment	02/05/2024

14. On April 24, 2024, after receiving additional information from Victim 1, the FBI opened an investigation.

Tracing of Victim 1's BTC Transactions

15. The FBI obtained details of Victim 1's transactions with Bitnukes directly from Victim 1 as well as through a review of Victim 1's civil complaint, which documented work performed by a company that consults on cryptocurrency-forensic investigations. FBI forensic accountants who are trained to conduct investigations involving cryptocurrency reviewed these sources of information and performed additional analysis using commercially available blockchain analysis tools.

16. The FBI learned that Victim 1 was directed to send his Bitnukes investment funds to three different BTC addresses throughout the duration of the scam. Victim 1's Bitnukes investments were funded through withdrawals he made at Crypto.com and Kraken accounts that Tara had instructed him to open.

17. From March 17 to April 14, 2023, Victim 1 sent approximately 16.76 BTC to wallet beginning with 3FZWGUig, which is a cluster of 4 addresses collectively referred to as a wallet. Commercial blockchain tracing tools identified 3FZWGUig as a scam tagged as bnukepd(.)vip. Based on my training and experience and conversations with FBI forensic accountants, I know that commercially available blockchain tracing tools cluster addresses based on heuristic algorithms that associate addresses to the same owner based on blockchain activity including common spending, change, and other publicly available data.

18. Blockchain analysis indicates that the total activity for wallet 3FZWGUig includes the receipt and withdrawal of approximately 72.3 BTC from October 29, 2022, to April 28, 2023. These transactions included Victim 1's investment intended for Bitnukes. Wallet 3FZWGUig sent funds either directly to a wallet beginning with 37Svi2w8, which is a cluster of 32 addresses, or to a wallet beginning with 32ST2HJH, which is a cluster of 10 addresses, before being remitted to wallet 37Svi2w8. Commercial blockchain tracing tools identified 37Svi2w8 as a scam tagged as bnukepz(.)vip.

19. On April 18, 2023, Victim 1 sent approximately 3.21 BTC to wallet beginning with 38X9H974, a cluster of five addresses. Blockchain analysis indicates that the total activity for wallet 38X9H974 includes the receipt and withdrawal of approximately 14.3 BTC from April 3 to July 5, 2023. These transactions included Victim 1's investment intended for Bitnukes. Wallet 38X9H974 sent approximately 73% of its funds directly to wallet 37Svi2w8.

20. From April 20 to April 21, 2023, Victim 1 sent approximately 10.87 BTC to wallet beginning with 37EAgLY9, a cluster of 4 addresses. Blockchain analysis indicates that the total activity for wallet 37EAgLY9 includes the receipt and transfer of approximately 25.6 BTC from

April 19 to June 3, 2023. These transactions included Victim 1's investment intended for Bitnukes. Wallet 37EAgLY9 sent approximately 99.9% of its funds directly to wallet 37Svi2w8.

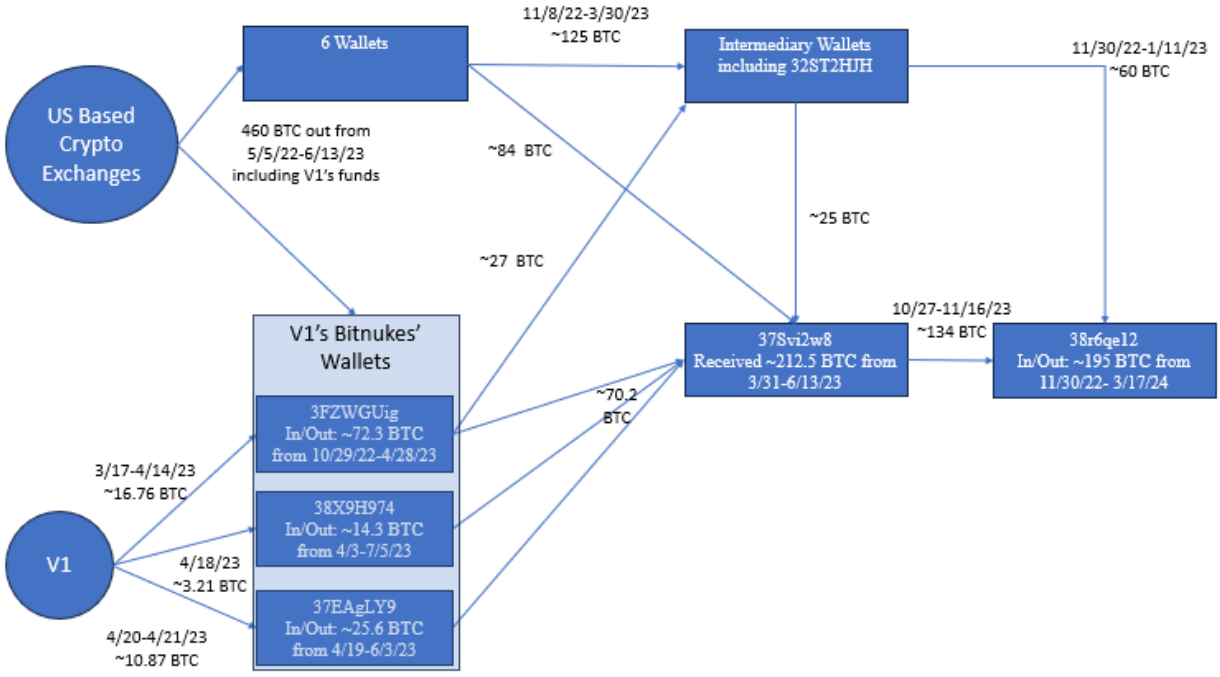
Further Tracing of Wallet 37Svi2w8

21. Blockchain analysis tools indicate wallet 37Svi2w8 is a cluster of at least 32 addresses likely under common control. From March 31 to June 13, 2023, wallet cluster 37Svi2w8 received approximately 212.5 BTC; approximately 70.2 BTC came from wallets into which Victim 1 transferred funds intended for Bitnukes and approximately 109 BTC came from other wallets. The remaining 33 BTC came from other unattributed private cryptocurrency addresses. These wallets were funded directly or indirectly from transfers originating at United States based cryptocurrency exchanges totaling approximately 460 BTC from May 5, 2022, to June 13, 2023, with the majority originating from Crypto.com.

22. Based on additional victim reporting and financial analysis, I believe this 460 BTC are likely scam proceeds. From April 2023 to November 2023, at least eight other victims filed online reports about Bitnukes with IC3.gov, the FBI's cyber complaint center. The 460 BTC originates primarily from Crypto.com transfers, which was the same cryptocurrency exchange utilized by Victim 1 and most other victims that filed reports with the FBI through IC3. Financial analysis shows that of the 460 BTC, approximately 109 BTC is directed through intermediary wallets and consolidated in wallet cluster 37Svi2w8, which was the same wallet used to consolidate Victim 1's Bitnukes investment. Financial analysis of details provided by one victim indicates they sent BTC to two addresses: to wallet cluster 3FZWGUig, to which Victim 1 also sent funds, and to an address which primarily received funds from Crypto.com and sent funds to 37Svi2w8. Based on financial analysis, my training and experience, and conversations with FBI forensic accountants,

wallet cluster 37Svi2w8 likely serves as a consolidation point for BTC obtained from victims of fraud.

23. Further analysis of intermediary wallets funded by the 460 BTC shows that from November 30, 2022, to January 11, 2023, approximately 60 BTC was eventually sent to a wallet beginning with 38r6qe12, which is a cluster of seven addresses. Wallet cluster 37Svi2w8 sent two transfers totaling approximately 134 BTC on October 27 and November 16, 2023, to 38r6qe12. From November 30, 2022, to March 17, 2024, these transfers comprised 99% of the funds received by wallet 38r6qe12, which appears to serve as a consolidation point for funds from 37Svi2w8 and other wallets funded by likely scam proceeds.

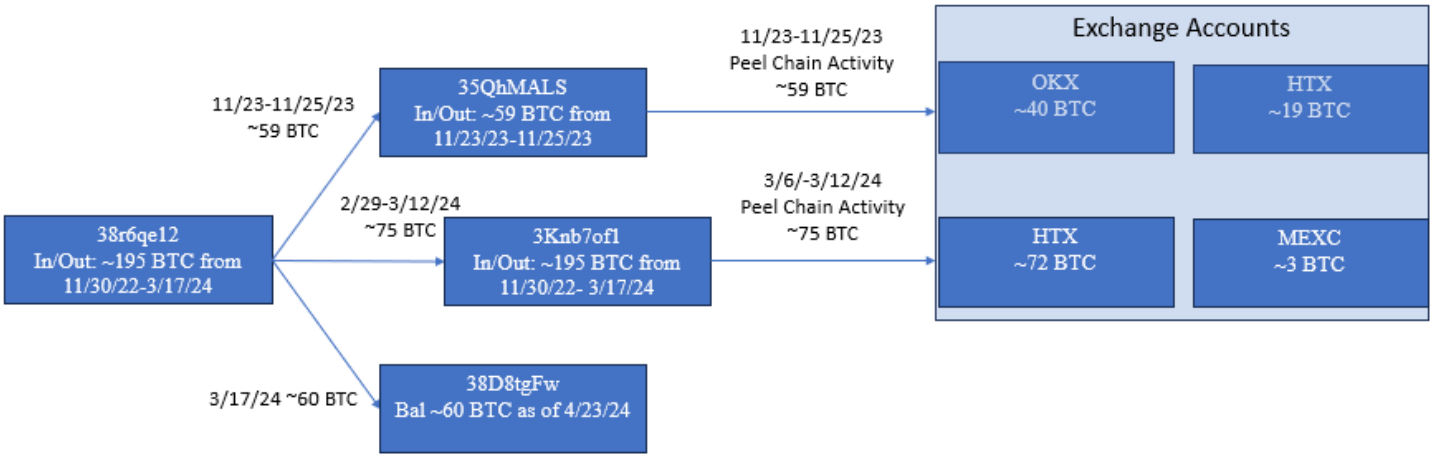


Further Tracing of Wallet 38r6qe12

24. Wallet cluster 38r6qe12 remitted nearly all the funds it received to three BTC addresses: address beginning in 35QhMALS, address beginning in 3Knb7of1, and address beginning in 38D8tgFw.

25. From November 23 to November 25, 2023, three transfers from wallet cluster 38r6qe12 totaling 59 BTC were initiated to address 35QhMALS. From November 23 to November 25, 2023, wallet address 35QhMALS then initiated several peel chains until approximately 40 BTC arrived at OKX and approximately 19 BTC arrived at HTX. A peel chain is a transaction pattern in which a small amount of BTC is sent to a destination address with the remaining BTC balance moving to a new BTC address, which is then repeated until all funds have been moved to a destination address. Based on my training and experience and conversations with FBI forensic accountants, peel chain transaction activity, is indicative of money laundering.

26. On March 3, 2024, two transfers from wallet cluster 38r6qe12 totaling 75 BTC were sent to wallet address 3Knb7of1. From March 6 to March 12, 2024, wallet address 3Knb7of1 then initiated peel chain transaction activity and ultimately sent approximately 72 BTC to HTX and approximately 3 BTC to MEXC, both cryptocurrency exchanges. On March 17, 2024, one transfer of 60.2 BTC was sent from wallet cluster 38r6qe12 to private wallet address 38D8tgFw where it remained as of April 23, 2024. On April 24, 2024, an FBI forensic accountant sent requests to OKX and HTX seeking account holder information for the ultimate destination of these funds.



OKX Records

27. On May 1, 2024, the FBI received a voluntary response from OKX that included account information for one OKX user, identified as user ID 460511322279437347, which revealed the account was created on June 30, 2023, by Yao Lutao (**OKX-Lutao 7347**). The records included subscriber information for the account holder, an email account, IP records, and transaction details. From November 23 to November 26, 2023, **OKX-Lutao 7347** received 26 deposits of BTC that totaled approximately 40 BTC, which ranged in amounts from 1 BTC to 2 BTC. Nearly all the funds **OKX-Lutao 7347** received were converted from BTC to USDT[2] and remitted to two wallets. From November 1 to November 25, 2023, **OKX-Lutao 7347** sent 47 transfers totaling approximately 1,699,815 USDT to a wallet beginning in TFF3DB83, and from June 30 to

[2] USDT is also called Tether, which is a stablecoin pegged to the value of the U.S. Dollar. Based on my training and experience and conversations with FBI forensic accountants, I know that cryptocurrency values are volatile and frequently fluctuate. Stablecoins exist to remove some of this volatility for cryptocurrency users. Tether's stability has helped the digital token become a preferred choice for fraudsters and money launderers.

November 23, 2023, **OKX-Lutao 7347** sent 7 transfers totaling approximately 81,670 USDT to a wallet beginning in TH1ELcCL.

28. **OKX-Lutao 7347** was also involved in Victim 1's civil complaint filed in the United States District Court for the Northern District of Florida. Victim 1 served OKX with a copy of the final judgment on or about February 8, 2024. On or about February 9, 2024, OKX acknowledged funds were frozen in **OKX-Lutao 7347**, but OKX required seizure process from U.S. law enforcement to release the funds. Records voluntarily provided to the FBI on May 1, 2024, indicate a balance of approximately 3.41 BTC remained in the account.

HTX Records

29. On July 1, 2024, the FBI received a voluntary response from HTX about the BTC sent to the exchange through peel chain activity. These records included information for three HTX users: User ID 453239327, created on June 29, 2023, by Yao Lutao (HTX-Lutao 9327); User ID 471251387, created on October 29, 2023, by Laura Kalaibekova (HTX-Kalaibekova 1387); and User ID 479409346, created on January 15, 2024, by Natalia Komrakova (HTX- Komrakova 9346). The records included subscriber information for the account holder, an email account, IP records, and transaction details.

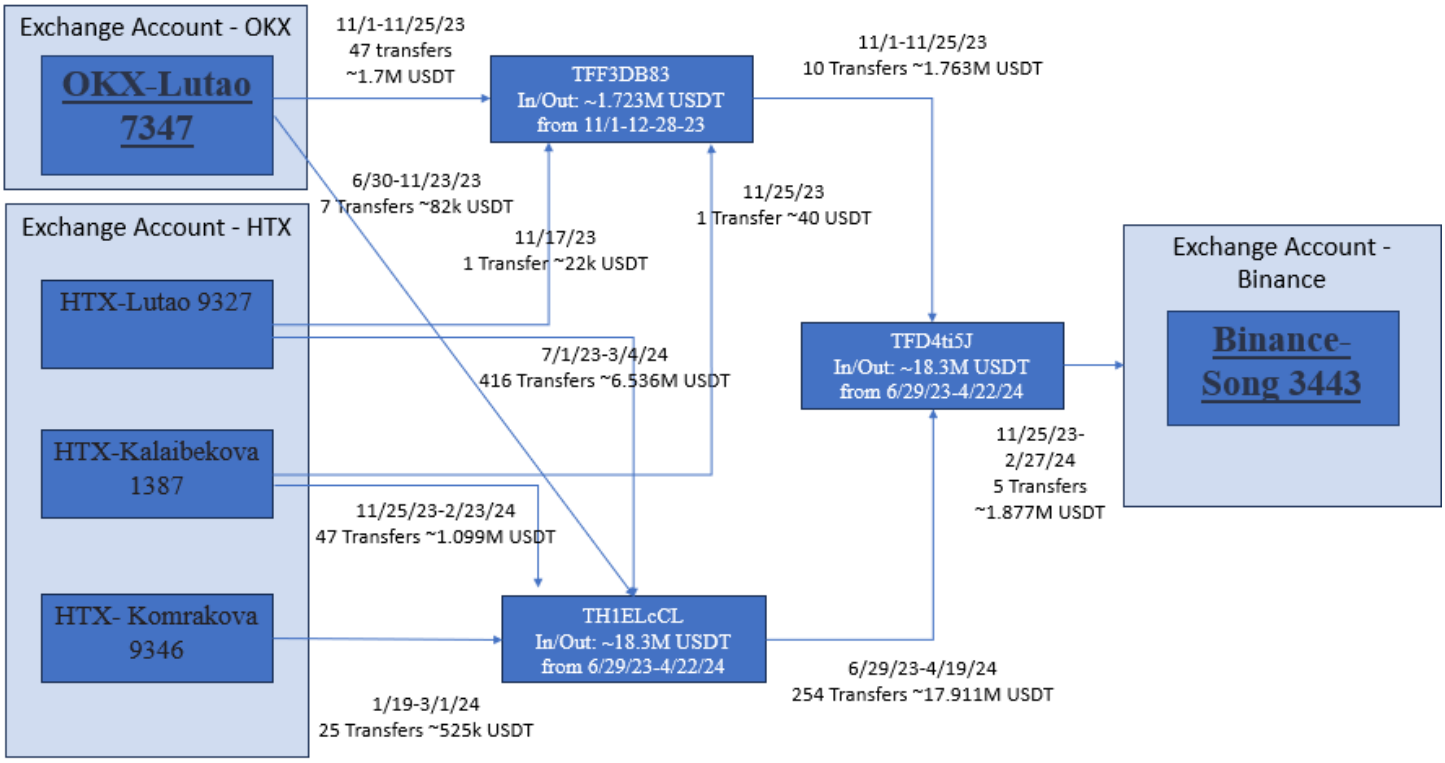
30. An FBI forensic accountant reviewed these HTX records and learned the accounts primarily received BTC deposits and withdrew amounts in USDT. On November 17, 2023, HTX-Lutao 9327 sent 21,901 USDT to TFF3DB83, which as described above, is also a wallet to which **OKX-Lutao 7347** sent multiple transfers. From July 1, 2023, to March 4, 2024, HTX-Lutao 9327 also sent 416 transfers totaling 6,536,226 USDT to TH1ELcCL, another wallet to which **OKX-Lutao 7347** sent multiple transfers. On November 25, 2023, HTX-Kalaibekova 1387 sent 40 USDT

to TFF3DB83, and from November 25, 2023, to February 23, 2024, sent forty-seven transfers totaling 1,099,045 USDT to TH1ELcCL. From January 19, 2024, to March 1, 2024, HTX-Komrakova 9346 sent twenty-five transfers totaling 525,352 USDT to TH1ELcCL.

31. Approximately 96% of all the funds received by TFF3DB83 from November 1 to December 28, 2023, originated from the four cryptocurrency exchange accounts described above that were likely funded by victims of fraud schemes. From November 1 to November 25, 2023, TFF3DB83 remitted 99% of the funds it received via ten transfers totaling 1,762,503 USDT to address beginning in TFD4ti5J.

32. Approximately 45% of all the funds received by TH1ELcCL from June 29, 2023, to April 22, 2024, originated from the four exchange accounts described above that were likely funded by victims of fraud schemes. From June 29, 2023, to April 19, 2024, TH1ELcCL remitted approximately 97% of the funds it received via 254 transfers totaling 17,910,929 USDT to TFD4ti5J. Based on my training and experience and conversations with FBI forensic accountants, TFD4ti5J appears to exist as a consolidation address for cryptocurrency that was likely acquired from victims of fraud and subsequently laundered through intermediary wallet addresses, peel chain activity, transfers to exchange accounts where it was converted from BTC to USDT, and subsequently transferred to additional intermediary wallet addresses.

33. From November 25, 2023, to February 27, 2024, TFD4ti5J initiated 5 USDT transfers totaling approximately $1,877,250 to Binance account User ID 111213443, created on April 4, 2021, by Nan Song **(Binance-Song 3443).**



34. On August 29, 2024, at the request of the FBI, Binance froze **Binance-Song 3443.** Binance notified Song that his accounts were frozen and provided him with my contact information. On August 29, 2024, Nan Song called the FBI Portland Field Office to speak with me. Nan Song wanted to know why his account was frozen and what could be done to unfreeze it.

Conversation with Binance-Song 3443 Account Holder Nan Song

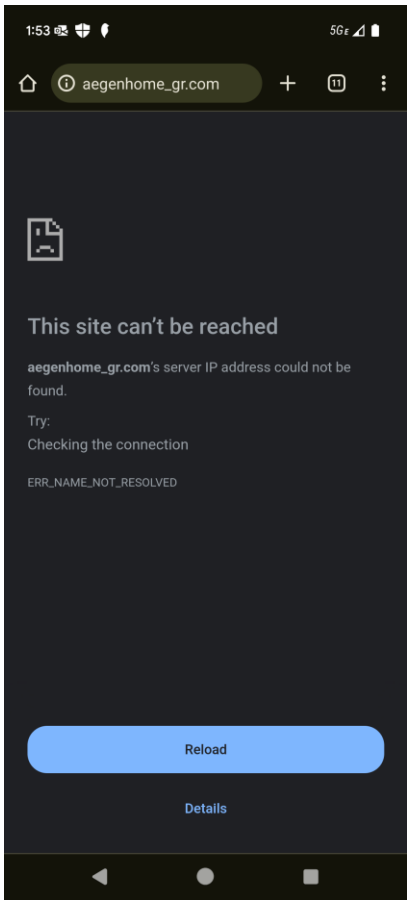
35. Song told me that **Binance-Song 3443** was his account, but the money was not his because it belonged to his clients. Song stated that he operates a real estate consulting business. Song was from China and first worked in the real estate consultancy business helping foreign clients trying to buy properties in Greece.

36. Song moved from China to Turkey in 2019 and started his own real estate consulting business in 2022 called PointTurkey. Song mainly served residential clients that were relocating their families to Turkey. Song received clients from real estate agents in China. Song had a website and attended trade shows every two to three months in China. Song's website was www.aegenhome_gr(.)com. Song said he met a lot of the real estate agents in person but could not remember any of their names or the companies they worked under. Later in the interview, Song told me that he had not met most of the agents in person. Song said he mainly communicated with agents via WeChat. Song later remembered one agent's name was Wenxian Huang.

37. Since most of Song's clients were from China, they were unable to transfer more than $50,000 to a foreign bank account. Song accepted USDT deposits from these clients and transferred their funds to Turkish bank accounts held in the name of his clients to get around China's transfer restrictions. Song did not know how his clients converted their local currency to USDT or where it came from.

38. One of the last clients Song worked with was X.L. Song was introduced to X.L. through a Chinese agent but could not remember the agent's name. Song said he met in person all of his clients that purchased properties because they had to travel to Turkey for fingerprinting and to receive their property title deed. Song picked them up at the airport or met them at their hotel in Turkey. Song sometimes booked their travel from Beijing to Istanbul. Song was not sure the number of clients he served but thought it was probably around 100. Song claimed to have support for every transaction that was conducted in his Binance account including the client's name, contact information, property address, Turkish e-Visa, and referring agent.

39. While on the phone with Song, I attempted to visit his website www.aegenhome_gr(.)com. I received a message that the site could not be reached and confirmed repetitively that I was visiting the correct URL. Song was unsure why the site was not available and stated he had not connected to it for some time.



40. At the conclusion of the interview, I requested Song send me his client's names, contact information, property address, Turkish e-Visa, and referring agent, for every transaction that was conducted in his Binance account. Song agreed to do so. I followed up with Song on August 29, 2024, and requested the documentation by the next day. On August 30, 2024, I received

emails from Song containing screenshots. The screenshots appear to be from a private wallet that depicts transactions on the blockchain.

41. The screenshots depict two transfers on June 22, 2024, for 379,900 USDT and 100 USDT, from an address beginning with TWpXF99y to an address beginning with TKY8hbmc. Song indicated in the email that the transactions were made for client L.L. for a property. Song also indicated he received the client from the Agent Suniver's Investment Group Limited.

42. Blockchain analysis indicates that the total activity for the recipient address, TKY8hbmc, includes the receipt and withdrawal of approximately 8,939,000 USDT from December 16, 2023, to August 30, 2024. Review of **Binance-Song 3443** indicates from February

28 to July 29, 2024, it received eight USDT transfers from address TKY8hbmc totaling approximately $6,875,098. Song provided me an email and screenshot which attributed TKY8hbmc as his Bitpie account. Bitpie is a multi-blockchain decentralized wallet. It allows users to receive, store, and send cryptocurrency while maintaining control of their assets.

43. Commercial cryptocurrency tracing tools do not presently attribute TKY8hbmc as a Bitpie wallet, however over time that can change. The four most recent deposits to **Binance-Song 3443** totaled approximately 3,531,449 USDT of which 98% came from TKY8hbmc. Further tracing from TKY8hbmc indicates these funds originated from 15 anonymous USDT addresses from June 26 to July 28, 2024, over 36 deposits ranging from 10 to 528,900 USDT. The three largest sources of these funds were three private USDT wallets addresses beginning TJ7X1ABV, TPHY2HTT, and TGFDH14C.

44. TJ7X1ABV sent 1,482,265 USDT in six transfers from July 18 to July 28, 2024, and financial analysis indicates TJ7X1ABV was indirectly funded by transfers from SWFT.pro bridge. According to Medium.com, SWFT.pro is a one stop cross-chain exchange platform that provides users with direct access to wallets and can complete cross-chain exchanges without registration and login. Cross-chain exchanges allow users to swap between cryptocurrencies. Based on my training and experience and conversations with FBI forensic accountants, cross-chain exchanges are frequently used for money laundering because they are difficult to track.

45. TPHY2HTT sent 521,018 USDT in four transfers from July 1 to July 22, 2024, and financial analysis indicates TPHY2HTT was indirectly funded by transfers from Binance, OKX, and HTX exchanges, however the most direct sources of funds were USDT private wallets.

46. TGFDH14C sent 410,000 USDT in two transfers on July 24, 202,4 and financial analysis indicates 76% of the total activity of TGFDH14C was directly funded from transfers from unknown OKX exchange accounts.

47. Based on my training and experience and conversations with FBI forensic accountants, if Song were operating an escrow type service for real estate purchases, investigators would expect to see large one-time transfers from unique addresses directly sourced from exchanges. However, review of **Binance-Song 3443** and Song's self-attributed Bitpie account do not exhibit this type of expected activity. Instead, investigators see frequent transfers routed through the same private USDT wallets on different dates which would be unusual for someone purchasing a house.

48. Investigators would also expect to see withdrawals from **Binance-Song 3443** from USDT to bank accounts denominated in Turkish lira. Investigators see no withdrawals to any bank accounts directly from **Binance-Song 3443.** Nearly all the outgoing activity is denominated in USDT.

49. Song provided no other additional details including contact information or e-Visas for any clients.

50. FBI forensic accountants also conducted Blockchain analysis on the other address that Song provided, TWpXF99y, and learned the following. On August 12, 2024, address TWpXF99y received one transfer of USDT valued at approximately $56,058.60 from an address beginning with TW3kpbKK. This address was identified as associated with ENTGCLUB.com and tagged a scam by commercial blockchain tracing tools.

51. An FBI forensic accountant reached out to the commercial blockchain tracing tool for any information on how ENTGCLUB.com was attributed as a scam. Personnel from the blockchain tracing tool responded as follows:

> The websites "ENTGCLUB.com" and "ENTGIL.com" are fake digital currency exchanges which we believe are associated with pig butchering scam activity. These two websites were identified by our team from larger research into pig butchering scam websites. This research involves targeting a known pig butchering website, and doing additional research on elements of the websites to find additional websites that match these characteristics. Many of these pig butchering websites are created via a "template" and have similar website characteristics.
>
> We created accounts on these websites (on 07/23/2024 for "ENTGCLUB.com" and "ENTGIL.com") and received the labeled deposit addresses to send funds, which we did not do, but victims did previously. The deposit address . . . was found to be utilized by both "ENTGCLUB.com" and "ENTGIL.com".

52. Based on my training and experience, I know that "pig butchering" is another term used to refer to a cryptocurrency investment fraud. Based on my training and experience, I also know that perpetrators of online fraud utilize money mules to help launder victim funds. Money mules can be witting or unwitting participants to a fraud. Money mules sometimes believe they are performing a job where they can work from home and earn money. Job tasks often involve the processing of payments, transfer of funds, or reshipment of products to facilitate the movement of money obtained through fraud from victims to criminals. Money mules are often instructed to lie and tell financial institutions or others that inquire that they have met the counterparty to their transaction in person when that is not true. I believe that Song is likely a money mule based on the evidence he claimed to have, versus what he provided me after our conversation.

53. On September 5, 2024, I applied to this court and received authorization from the Honorable Judge Stacie Beckerman to seize 3,086,226.36 USDT stored in **(Binance-Song 3443)** and 3.41 BTC stored in **(OKX-Lutao 7347),** via case 3:24-mc-901.

54. On September 5, 2024, I obtained and served seizure warrants to Binance and OKX. On September 6, 2024, Binance acknowledged receipt of the seizure warrant and communicated their intent to process the seizure.

55. On September 3, 2024, and September 13, 2024, I received emails from Nan Song who inquired about the status of his case. No further communication has occurred with Nan Song.

56. On October 22, 2024, a government-controlled public cryptocurrency address received 3,086,213.86 USDT from Binance, which represented the seized funds stored in **(Binance-Song 3443)**, less transaction fees.

57. On October 22, 2024, OKX, a Republic of Seychelles entity, acknowledged receipt of the seizure warrant and communicated they consider seizure requests made with foreign courts on a voluntarily basis. On October 29, 2024, I provided all the information requested by OKX to process the seizure, including a government-controlled public cryptocurrency address, and received no response.

58. On November 8, 2024, I followed up with OKX regarding the status of the seizure and received no response.

59. On December 6, 2024, I again followed up with OKX and received a response on December 8, 2024, that they were still processing the seizure. As of December 9, 2024, no funds had been transferred to the government-controlled public cryptocurrency address from OKX.

Conclusion

60. Based on the foregoing information, I have probable cause to believe, and do believe, that the 3,086,213.86 USDT stored in a government-controlled public cryptocurrency wallet represents the funds seized from **(Binance-Song 3443),** less transaction fees, and 3.41 Bitcoin (BTC), or equivalent cryptocurrency, valued at approximately $331,051.05 on December 9, 2024, stored in an OKX account with User ID 460511322279437347 held in the name of Yao Lutao (**OKX-Lutao 7347**), is subject to seizure pursuant to 18 U.S.C. §§ 981(b), and subject to forfeiture pursuant to 18 U.S.C. §§ 981(a)(1)(A) & (C) as monies involved in transactions or attempted transactions or traceable to money laundering offenses in violation of 18 U.S.C. § 1956(a)(1)(B)(i) (concealment money laundering) and 18 U.S.C. § 1957 (unlawful monetary transactions in excess of $10,000), and is property constituting or derived from proceeds obtained, directly or indirectly, from a violation of 18 U.S.C. § 1343 (wire fraud).

I declare under penalty of perjury that the foregoing is true and correct pursuant to 28 U.S.C. §1746.

Executed this 13 day of January 2025.

/s/ Eric Hiser
ERIC HISER
Special Agent
Federal Bureau of Investigation